REMARKS

Claims 1-14 are pending. The Examiner's reconsideration of the rejections is respectfully requested in view of the remarks.

Information Disclosure Statement

The Examiner indicated that non-English references cited in the previously submitted IDS were not considered for lack of a concise explanation of their relevance. Attached hereto is second IDS giving a concise explanation of the relevance of the non-English references. The Examiner's consideration of the references is respectfully requested.

Rejections Under 35 USC 103(a)

Claims 1-14 have been rejected under 35 USC 103(a) as being unpatentable over USPN 5,473,693 to Sprunk in view of US Patent Publication No. 2002/0048364 to Gilgor et al. The Examiner stated essentially that the combined teachings of Sprunk and Gilgor teach or suggest all of the limitations of Claims 1-14.

Claims 1, 7 and 9 are the independent claims.

Claims 1 and 9 recite "the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion."

Claim 7 claims, *inter alia*, "cryptographically converting, substantially simultaneously, a digital input data block into a first digital output data block nonlinearly, based on an input of a set of encryption keys and an inverse of the digital input data block into a second digital output data block nonlinearly, based on an inverse of the encryption keys".

Claims 1 and 9

Sprunk teaches applying a function to one or more inputs and/or an output of a processor (see FIG 2 and col. 3, line 51 to col. 4, lines 14). Sprunk teaches only a single processor for performing encryption (see FIG 2). In the Response to Arguments section of the Final Office Action the Examiner states essentially that the claim does not explicitly recite two encryption devices. Respectfully, Claims 1 and 9 recite "the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion." Thus, two encryption devices are clearly claimed. Sprunk does not teach or suggest two encryption devices, much less that "the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion" as claimed in Claims 1 and 9. Therefore, Sprunk fails to teach or suggest all the limitations of Claims 1 and 9.

Gilgor teaches methods for parallel block encryption (see Abstract). Gilgor does not teach or suggest that "the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion" as claimed in Claims 1 and 9. Upon review of Gilgor it is apparent that while the disclosure refers to modes and components, the disclosure is completely devoid of support for a hardware implementation, much less first and second N-round DES devices as claimed in Claims 1 and 9. Therefore, Gilgor fails to cure the deficiencies of Sprunk.

The combined teachings of Sprunk and Gilgor teach a single processor for parallel processing of a data block. The combined teachings of Sprunk and Gilgor fail to teach or suggest that "the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion" as claimed in Claims 1 and 9.

Claims 1 and 9 are believed to be allowable for additional reasons; the combined

teachings of Sprunk and Gilgor fail to teach or suggest that "the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion process" as claimed in Claim 1 and essentially as Claimed in Claim 9. For example, Sprunk teaches that one of a data block, a cryptographic key and an output are inverted (see Claim 1, col. 5, lines 45-53), wherein a nonlinear function is applied once (see col. 5, line 53 to col. 6, line 5). Further still, Sprunk is clear that complementarity (wherein the data block and cryptographic key are both inverted as claimed in Claims 1 and 9) is to be avoided as a compromise of security nowhere. Thus, Sprunk teach or suggest the claimed simultaneous cryptographic conversion process where a first device processes an input block and a second device processes an inverted version of the input block.

Gilgor teaches data encryption operations performed on blocks of an input plaintext string in parallel (see paragraph [0024]). Similar to Sprunk, Gilgor does not teach or suggest encryption of the digital input data block and an inverse of the digital input data block. Indeed, Gilgor emphasizes that only one processing pass is required over the data or message (see paragraph [0022]). Clearly then, Gilgor does not teach or suggest the claimed simultaneous cryptographic conversion process where a first device processes an input block and a second device processes an inverted version of the input block. Therefore, Gilgor fails to cure the deficiencies of Sprunk.

The combined teachings of Sprunk and Gilgor teach parallel processing of data blocks, wherein one of the data block, the cryptographic key and the output are inverted. The combined teachings of Sprunk and Gilgor fail to teach or suggest that "the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion" as claimed in Claims 1 and 9.

Claim 7

Sprunk teaches that one of a data block, a cryptographic key and an output are inverted (see Claim 1, col. 5, lines 45-53), wherein a nonlinear function is applied once (see col. 5, line 53 to col. 6, line 5). Sprunk fails to teach or suggest "cryptographically converting, substantially simultaneously, a digital input data block into a first digital output data block nonlinearly, based on an input of a set of encryption keys and an inverse of the digital input data block into a second digital output data block nonlinearly, based on an inverse of the encryption keys" as claimed in Claim 7. Sprunk teaches that complementarity (wherein the data block and cryptographic key are both inverted as claimed in Claim 7) is to be avoided as a compromise of security.

Gilgor teaches methods for parallel block encryption (see Abstract and paragraph [0024]). Gilgor fails to teach or suggest "cryptographically converting, substantially simultaneously, a digital input data block into a first digital output data block nonlinearly, based on an input of a set of encryption keys and an inverse of the digital input data block into a second digital output data block nonlinearly, based on an inverse of the encryption keys" as claimed in Claim 7. As shown above, Gilgor emphasizes that only one processing pass is required over the data or message (see paragraph [0022]), thus teaching away form the claimed method. Therefore, Gilgor fails to cure the deficiencies of Sprunk.

The combined teachings of Sprunk and Gilgor teach a parallel encryption of different blocks (see Gilgor), wherein inputs and/or an output of the different blocks may be treated by a nonlinear function of Sprunk. The combined teachings of Sprunk and Gilgor fail to teach or suggest that "cryptographically converting, substantially simultaneously, a digital input data block into a first digital output data block nonlinearly, based on an input of a set of encryption keys and an inverse of the digital input data block into a second digital output data block nonlinearly, based on an inverse of the encryption keys" as claimed in Claim 7. The Examiner's

9

reconsideration of the rejection is respectfully requested.

Claims 2-6 depend from Claim 1. Claim 8 depends from Claim 7. Claims 10-14 depend from Claim 9. The dependent claims are believed to be allowable for at least the reasons given for the respective independent claims. Reconsideration of the rejection is respectfully requested.

For the forgoing reasons, the present application, including Claims 1-14, is believed to be in condition for allowance. The Examiner's early and favorable action is respectfully urged.

Respectfully submitted,

Dated: January 31, 2008   By:

Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicants

Mailing Address:
F. CHAU & ASSOCIATES, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889